The best way, to learn and apply cryptography

The CrypTool project is about making the sometimes daunting subject of cryptography more accessible and easy to understand. It is the most comprehensive cryptography learning tool worldwide.

**What you will learn…**
- Cryptography’s place in modern communications
- CrypTool project history
- Available CrypTool versions and some features

**What you should know…**
- Basic understanding of mathematics
- Basic understanding of cryptography
- Using the Internet

We would like to introduce to you CrypTool (CT1) and the two successors, CrypTool 2 (CT2) and J CrypTool (JCT), using in each case a very small extract of their capabilities. Each project is open-source and available for free.

The history of cryptography goes back more than 2000 years; secret communication has always been important – mostly for military and political reasons. The breakthrough of cryptography followed the broadening usage of the Internet. In modern days cryptography has evolved into a mathematically characterized science that most people use everyday without even realizing it. Cryptography is used in our mobile phones, in ATM cards, Pay TV, secure e-mail or online shopping and much more. The four objectives that cryptography is addressing today are confidentiality, authentication, integrity and non-repudiation of digital data. Applications fulfilling these objectives ease our everyday lives, such as secure online banking or non-reproducible digital signatures that verify and protect important documents. This allows us to save time or to further eliminate bureaucracy. Cryptography has become such a vital technology in modern communications and is nevertheless barely known to most people.

Today, cryptography is not only interesting for business and commercial use. Recent political developments like the inspection of laptops or other electronic devices while crossing state borders make cryptography more and more interesting for each and everyone of us that value and cherish our rights of privacy. The technology to ensure privacy is there – it’s free and it’s secure. On the other hand, it is almost impossible to have a one hundred percent secure computer system due to its complexity and ever evolving technologies. Cryptography applied correctly, can secure valuable data so it is impossible to be accessed by a third party. This includes yourself if you forget your password. It is important to understand that a lost password may mean to lose valuable data. Cryptography gives us the tools to write secure e-mails and secure our private conversations in social networks or instant messengers, but is rarely used by private persons.

The past has shown that security through obscurity and proprietary cryptography can’t really be trusted. Many cryptography researchers agree that only if a cryptographic algorithm is open and available to the cryptographic community it can be analyzed and tested.

**MysteryTwister C3 – Level I challenge number sequence**

What is the next number in this sequence?


How did you find the solution?

Visit the MTC3 homepage to discuss and for more challenges: http://www.mysterytwisterc3.org/
The best way, to learn and apply cryptography

After the company-internal project ended, and thanks to the efforts of Prof. Bernhard Esslinger and the support of board member Hermann-Josef Lamberti, it was handed over to the Internet community and first released as freeware in the year 2000. In 2003 it became open source hosted by the University of Darmstadt. Since then, the CrypTool project evolved into the most comprehensive cryptography e-learning platform available today. Additionally the CrypTool programs can be used as well proven encryption programs. The project is ever-evolving and has now diversified into three software implementations, each with unique abilities, objectives and technologies behind them. For each project we put the numbers of it’s downloaded setup files for 2010 (containing the whole package) into the Tables 1, 2 and 3.

**CrypTool 1**
(Requirements: Windows XP or later)

CT1 is currently the most complete and mature CrypTool variant, implementing nearly all state-of-the-art cryptography functions and offering a comprehensive online documentation. CT1 is written in C++ and runs only under Win32 OS.

Each function implemented is using a simple graphical interface. The online help is understandable without a deep knowledge of cryptography. It also contains a learning tool for number theory, a secure e-enhancements to verify that it is really secure. Otherwise, a proprietary closed algorithm may contain serious flaws that, when exposed later, will require significant costs to eliminate the security risk. An example of such a situation is the MIFARE chip, which was used in millions of devices in the transportation industry before being compromised. Another example is the encryption used in wireless (DECT) phones – now your neighbor may find out when you complain about him.

Because many cryptographic algorithms are open, everyone has access to modern cryptographic technologies and all of us have the chance to learn about them and how to use them correctly.

The goal of the CrypTool project is to help and encourage people to understand cryptography and the underlying technologies. It demonstrates current state-of-the-art cryptographic technologies, as well as cryptanalysis and known attacks against cryptographic systems.

The CrypTool project is also trying to consolidate research and software implementations that has been done by individuals mostly from universities and companies, so others can learn from it. It gives their students a unique opportunity to contribute their code (e.g. software written for a thesis) to a project where it is maintained and used by others around the world rather then just disappearing into the ether.

The CrypTool project started in a large financial institution in 1998. It's original purpose was internal training, to raise awareness about cryptography and encourage developers to use standardized cryptographic libraries instead of self made software. It was also used as a reference to confirm other software implementations.

![Figure 1. CrypTool 1 – main window](image1)

![Figure 2. CrypTool 1 – password quality meter](image2)
mail demonstration and visualizations of many different encryption algorithms. CT1 is available in 5 different languages: English, German, Polish, Serbian and Spanish. One feature in CT1 that is useful for almost anyone to try is the password quality meter (PQM see Figure 2). There are tons of similar tools that can be found online, but most of them ask you to share your password and send it to a server. Potentially you risk that someone is logging your passwords for later use. The PQM built into CT1 keeps everything locally on your computer and does more than simply counting how many characters you enter and calculate statistics. It also checks the entered passwords against a dictionary (that can also be configured).

You may ask yourself what a password check has to do with cryptography. Even if you use the best encryption algorithms there today, they often rely on a secure (hard to guess/find) password, large prime or random numbers to reach their full potential of being unbreakable.

In 2007, the requirements of the CT1 user community were gathered in a big survey and the preferences of the potential developers were looked at. The result was that the two successors of CT1 both are based on a pure-plugin architecture – one using .NET and C#, and the other using Eclipse, Java and RCP.

**CrypTool 2**
(Requirements: Windows XP or later, .NET 4.0)

CT2 is the first modern successor that uses state-of-the-art development techniques and goes a completely new way in didactic learning. CT2 follows the model of visual programming and offers all components using Microsoft’s Office 2007 user interface design guideline, providing a consistent and rich user experience. The visual programming model enables the user to combine an extended set of functions instead of being limited to just one function at a time. The vector-oriented GUI design is based on the Windows Presentation Foundation (WPF) and gives users the ability to scale the current view at will. It is being hosted by the University of Duisburg. The development is lead by Dr. Arno Wacker.

One very interesting function that has been implemented recently is the support for distributed computing. CT2 is able to establish ad-hoc peer-to-peer communications using sockets which are tightly integrated into the visual programming model. The CrypTool 2 server is also able to get notifications as soon as a new connection is established. This allows the users to start up a peer-to-peer connection at any time, while the server can be established in one single click and is available at all times.

In addition to the visual and interactive features, CrypTool 2 offers a large number of tutorials and a learning center with over 500 exercises. These exercises are designed to be easily integrated into different courses and educational programs. They are directly linked to the visual programming model and can be used to test and verify the knowledge and understanding of the users.

The CrypTool 2 project is open-source and is licensed under the GNU General Public License (GPL). The development is supported by several universities and research institutions, and the project is continuously improved and extended with new features and enhancements. The CrypTool 2 community is active and engaged, with regular updates and releases, as well as frequent contributions from the users themselves. The CrypTool 2 project is dedicated to providing high-quality tools for education and research in the field of cryptography and information security.
peer networks in order to speed up computing intensive tasks. If you are interested in prime numbers, CT2 has a standalone function build in, which dynamically visualizes different attributes and properties about primes. One feature that we would like to introduce to you is CT2’s modular design. It offers a toolbox with basic functions on the left side. These functions can be combined in projects to implement cryptographic protocols, build work-flows and test them against different analysis tools. CT2 can execute these workflows step by step. Teachers can use this to prepare tasks for their students, thus better utilizing the limited time available in a class. CT2 is currently available as beta 3 in German and English.

In CT2, more than 100 template-projects are deployed to illustrate how the functions can be used. Figure 4 shows how a pseudo-random number stream can be generated using the LFSR functions.

Table 2. CrypTool 2 – Downloaded around 44 000 times in 2010

<table>
<thead>
<tr>
<th>CT2</th>
<th>Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 2010</td>
<td>5,496</td>
</tr>
<tr>
<td>Nov 2010</td>
<td>5,161</td>
</tr>
<tr>
<td>Oct 2010</td>
<td>4,377</td>
</tr>
<tr>
<td>Sep 2010</td>
<td>3,681</td>
</tr>
<tr>
<td>Aug 2010</td>
<td>2,664</td>
</tr>
<tr>
<td>Jul 2010</td>
<td>2,480</td>
</tr>
<tr>
<td>Jun 2010</td>
<td>2,427</td>
</tr>
<tr>
<td>May 2010</td>
<td>3,231</td>
</tr>
<tr>
<td>Apr 2010</td>
<td>4,612</td>
</tr>
<tr>
<td>Mar 2010</td>
<td>3,863</td>
</tr>
<tr>
<td>Feb 2010</td>
<td>3,492</td>
</tr>
<tr>
<td>Jan 2010</td>
<td>2,233</td>
</tr>
<tr>
<td>Sum 2010</td>
<td>43,717</td>
</tr>
</tbody>
</table>

Figure 6. JCrypTool – elliptic curve cryptography visualization
JcrypTool
(Requirements: Java run-time environment 1.6 or later)
JCT is CT2’s sibling. It’s also a successor of CT1, but
with other objectives than CT2. The main requirement
that it fulfills is platform independence, so it runs under
Windows, Linux as well as under MacOSX. JCT is
also being developed as an open-source project. It is
based on the Eclipse Rich Client Platform (RCP). It
enables students, teachers, developers, and anyone
else interested in cryptography to apply and analyze
cryptographic algorithms in a modern and easy-to-use
application. It uses both BouncyCastle and FlexiProvider
as crypto providers. Thanks to FlexiProvider, it offers
not only the algorithms which already passed the
standardization, but also some current research
algorithms mainly from the post quantum research field.
JCT Release Candidate 4 (RC4) is currently available
in German and English. It is hosted on SourceForge –
project lead is Dominik Schadow. JCT’s average ranking
on SourceForge is in the top 700-3000 (of the 180,000
registered projects).

JCT supports combining algorithms in cascades in
order to check and invent new variants of ciphers.
One of the currently 15+ visualizations build into JCT
is the elliptic curve cryptography (ECC) demonstration.
ECC is an interesting technology that can use much
smaller keys than RSA while being as secure (512 bits
with ECC equals the security of a 15,260 bit RSA key).

This is especially interesting for devices that don’t have
enough storage for large keys, e.g. in wireless sensor
networks. The concept behind ECC operations is
shown on the screen shot in Figure 6 with real numbers,
but you can also use elliptic curves on other sets like the
discrete field over p and the field over $2^m$.

**Related projects CT-Online, MTC3 and CT-Mobile**
The CrypTool project is a great success story and good
example for what open source and cooperative work of
different universities and companies can achieve. There
are further related projects like CrypTool-Online, which
offers the ciphers and functions directly in the browser
without any local installation. CrypTool-Mobile provides
this front-end for modern smartphones.

Another related project that just started is the
online crypto contest MysteryTwister C3, where you
can check your cryptography skills against others,
get listed in a global hall-of-fame and discuss your
attempts in a moderated forum. Currently around
1800 users are registered. The challenges come from
different authors, currently from Europe and the US.

**An open call to everyone interested**
Cryptography is all around us and I hope that we can
encourage more people to learn about this fascinating
science. Visit the official CrypTool website and take
a look at the project presentation to learn about all
the capabilities built into CrypTool. The CrypTool
project deeply appreciates any further contribution,
constructive criticism and feedback regarding our
current releases. You are welcome to join! Currently
more than 50 individuals world wide support the
project (some of the individuals were willing to offer
information about themselves publicly, see the map
continue its evolution and hopefully help more people
to learn about cryptography.

**ARKADIUS C. LITWINCZUK**
The author works as an IT-Security consultant and developer
in the area of cryptography.
Contact the Autor:
Arkadius.Litwinczuk@gmail.com
ID THEF

GUARDING AGAINST IDENTITY THEFT

THE BEST WAY TO LEARN AND APPLY CRYPTOGRAPHY

ANALYSIS OF A SCAM

SECURE ENV FOR PT

KNOWING VOIP – PART III

BLUETOOTH MICE CAN LEAK YOUR PASSWORDS

CHOOSING AN IDS/IPS ENGINE

PLUS

IDENTITY PROOF YOUR PERSONAL DATA

BY JULIAN EVANS